苏州大学实验报告

院、系	计算机学院	姓名	朱金涛	学号	2327406014
课程名称	计算机网络				
指导教师	高国举		实验完成日期		2025 年 10 月 31 日

实验名称：地址解析协议（ARP）

一、 实验目的

1. 掌握 ARP 协议的报文格式

2. 掌握 ARP 协议的工作原理

3. 理解 ARP 高速缓存的作用

4. 掌握 ARP 请求和应答的实现方法

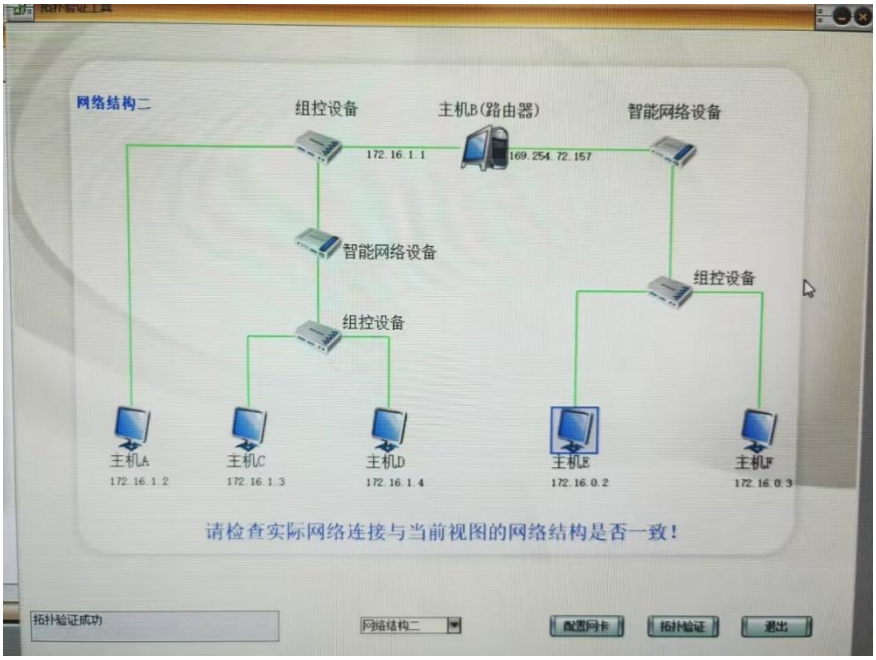
5. 掌握 ARP 缓存表的维护过程

二、 实验步骤

练习 1：领略真实的 ARP（同一子网）

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。本练习将主机 A、B、C、D、E、F 作为一组进行实验。

验证网络拓扑结果如下：



1. 主机 A、B、C、D、E、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP、ICMP）。

2. 主机 A、B、C、D、E、F 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。

3. 主机 A ping 主机 D（172.16.1.4）。

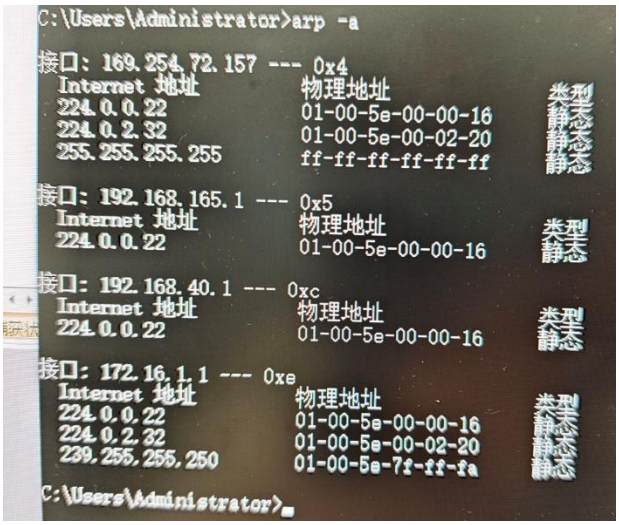
4. 主机 E ping 主机 F（172.16.0.3）。

5. 主机 A、B、C、D、E、F 停止捕获数据，并立即在命令行下运行“arp -a”命令查看 ARP 高速缓存。

主机 A：

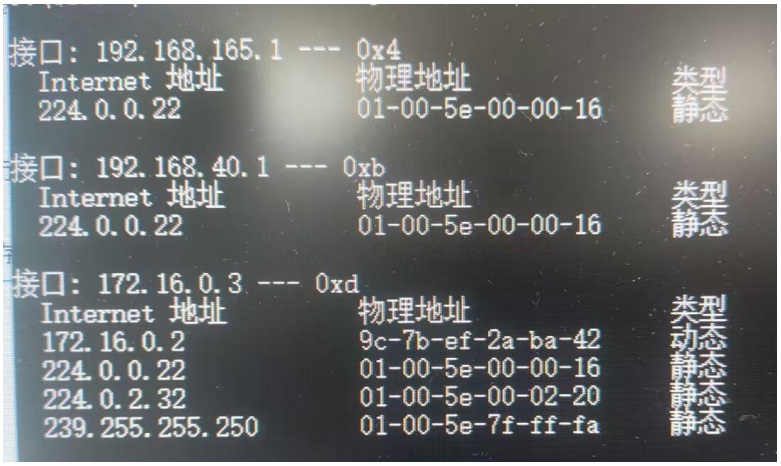
```
C:\Users\Administrator>arp -a

接口: 192.168.165.1 --- 0x4
  Internet 地址         物理地址              类型
  224.0.0.22            01-00-5e-00-00-16     静态

接口: 192.168.40.1 --- 0xb
  Internet 地址         物理地址              类型
  224.0.0.22            01-00-5e-00-00-16     静态

接口: 172.16.1.2 --- 0xd
  Internet 地址         物理地址              类型
  172.16.1.4            9c-7b-ef-2a-b9-bd     动态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.2.32            01-00-5e-00-02-20     静态
```

主机 B:



…（此处略显冗余，我就不把 C, D, E 贴上了。）

主机 F：



● ARP 高速缓存表由哪几项组成?

答:

- **状态**：标记当前条目的处理进度。取值包括 **FREE**（已过期/超时失效）、**PENDING**（已发出请求但尚未收到应答）、**RESOLVED**（已获得应答并完成解析）。
- **硬件类型 / 协议类型 / 硬件地址长度 / 协议地址长度**：与 ARP 报文首部中的对应字段一致，含义与编码规则与 ARP 标准相同。
- **接口号**：指路由器上承载该条目的具体接口编号，用于区分从哪个接口发起/接收。
- **队列号**：ARP 会为等待地址解析的报文维护多个排队队列；该编号表明条目所在的队列。面向同一目标的报文通常进入同一队列集中等待。
- **尝试**：该条目已经发送 ARP 请求的次数计数。
- **超时**：条目可存活的时间（秒）。到时未成功则条目失效或转为 FREE 状态。
- **硬件地址**：目标的二层地址（如 MAC）。在尚未收到 ARP 应答前保持为空，收到应答后填入。
- **协议地址**：目标的高层协议地址（如 IP 地址），用于指明需要解析成二层地址的对象。

● 结合协议分析器上采集到的 ARP 报文和 ARP 高速缓存表中新增加的条目，简述 ARP 协议的报文交互过程以及 ARP 高速缓存表的更新过程。

- 场景说明：本机 F 的 IP 是 172.16.0.3，主机 E 的 IP 是 172.16.0.1。E 需要把一个 IP 数据报（这里是 ICMP）发给 F，但暂时不知道 F 的 MAC。

1. 提取目的地址

主机 E 的 ARP 模块在收到待发送的 IP 数据报后，先取出目的 IP（即 F 的 172.16.0.3）。

2. 查询本地 ARP 缓存

E 在自己的 ARP 表中查找是否已有“F 的 IP → MAC”的条目；若已存在，直接用该 MAC 封装二层帧即可。

3. 发起地址解析

没查到映射时，E 在局域网内广播一个 ARP 请求报文：报文里带上发送方的 IP/MAC（E 自己），并给出目标的 IP（F 的 172.16.0.3），询问“谁是这个 IP，请把你的 MAC 告诉我”。

4. 等待应答

E 进入等待状态，准备接收对应的 ARP Reply。

5. 接收应答/失败处理

若 E 收到来自 F 的 ARP 应答，则进入下一步；如果超时仍未收到，则本次解析失败（通常会按重试策略再发 ARP，直到次数用尽）。

6. 完成映射与发送

E 从应答中取出 F 的 MAC，将“172.16.0.3 → 目标 MAC”写入本地 ARP 表；随后用这个 MAC 作为二层目的地址，把原本的 IP 数据报封装成以太网帧并发送出去。至此，对 F 的 ARP 解析完成。

练习 2：编辑并发送 ARP 报文（同一子网）

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1. 在主机 E 上启动协议编辑器，并编辑一个 ARP 请求报文。其中：

MAC 层：

目的 MAC 地址：设置为 FFFFFF-FFFFFF

源 MAC 地址：设置为主机 E 的 MAC 地址

协议类型或数据长度：0806

ARP 层：

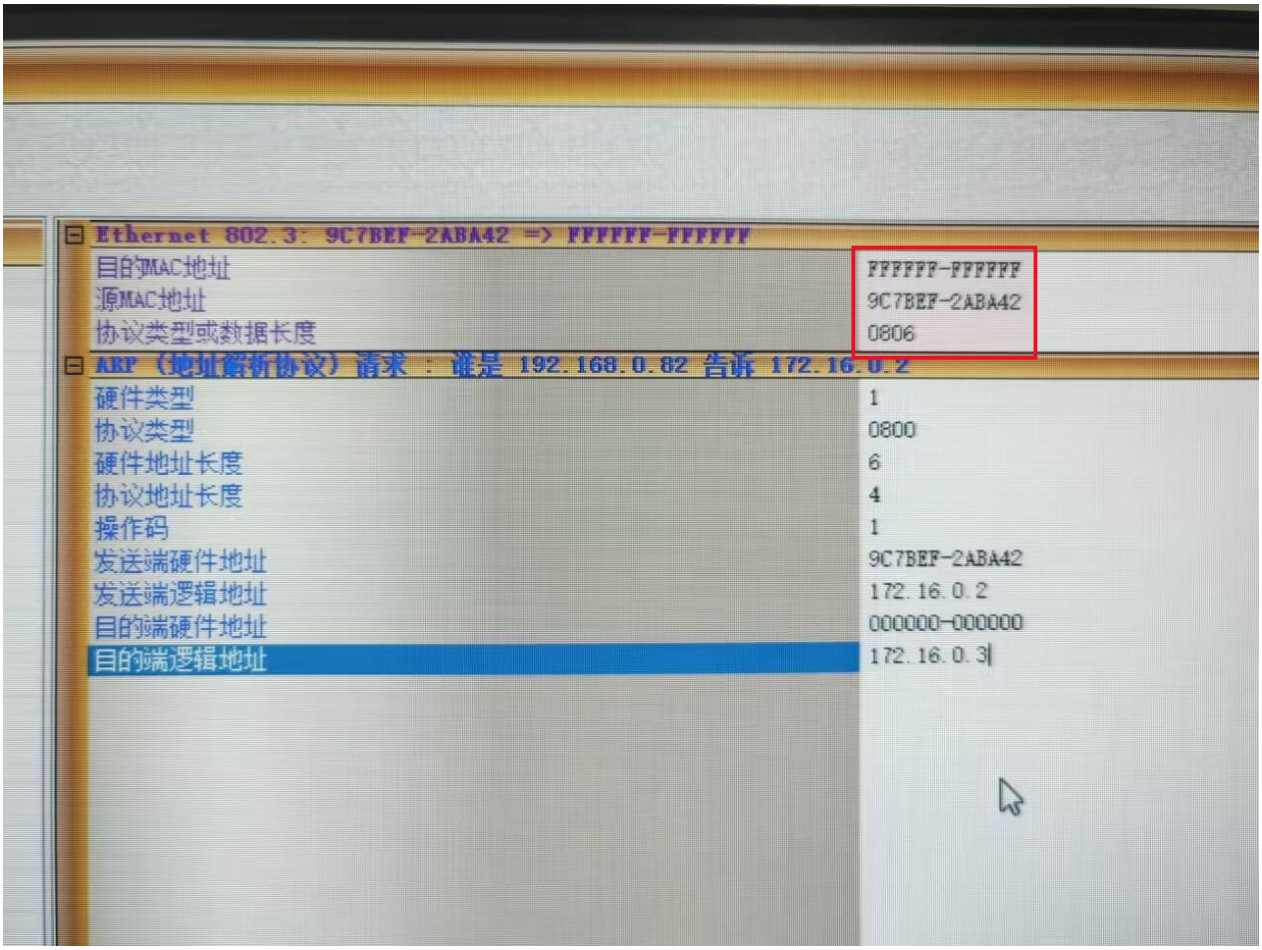
发送端硬件地址：设置为主机 E 的 MAC 地址

发送端逻辑地址：设置为主机 E 的 IP 地址（172.16.0.2）

目的端硬件地址：设置为 000000-000000

目的端逻辑地址：设置为主机 F 的 IP 地址（172.16.0.3）

主机 E 编写的帧结果图如下：



如图中红框所示，已按照实验要求设置了源/目的 MAC 地址、数据帧长度（0806）。

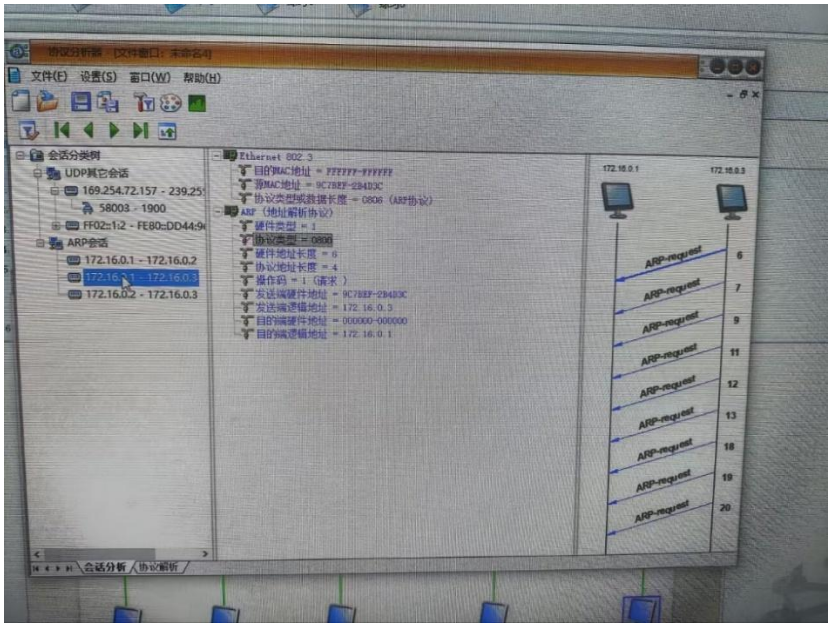
2. 主机 B、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP 协议）。

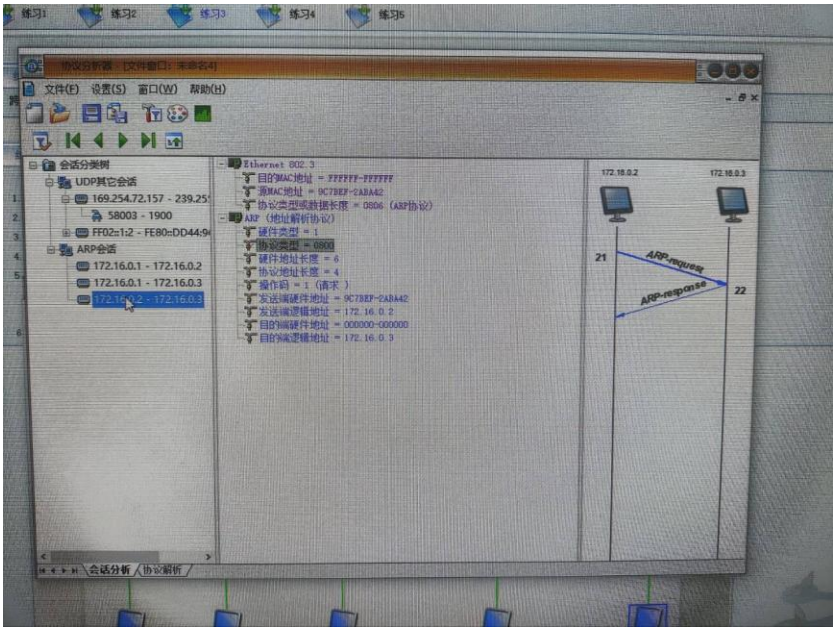
3. 主机 B、E、F 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。主机 E 发送已编辑好的 ARP 报文。

4. 主机 B、F 停止捕获数据，分析捕获到的数据，记录 ARP 报文交互过程。

- 记录实验结果

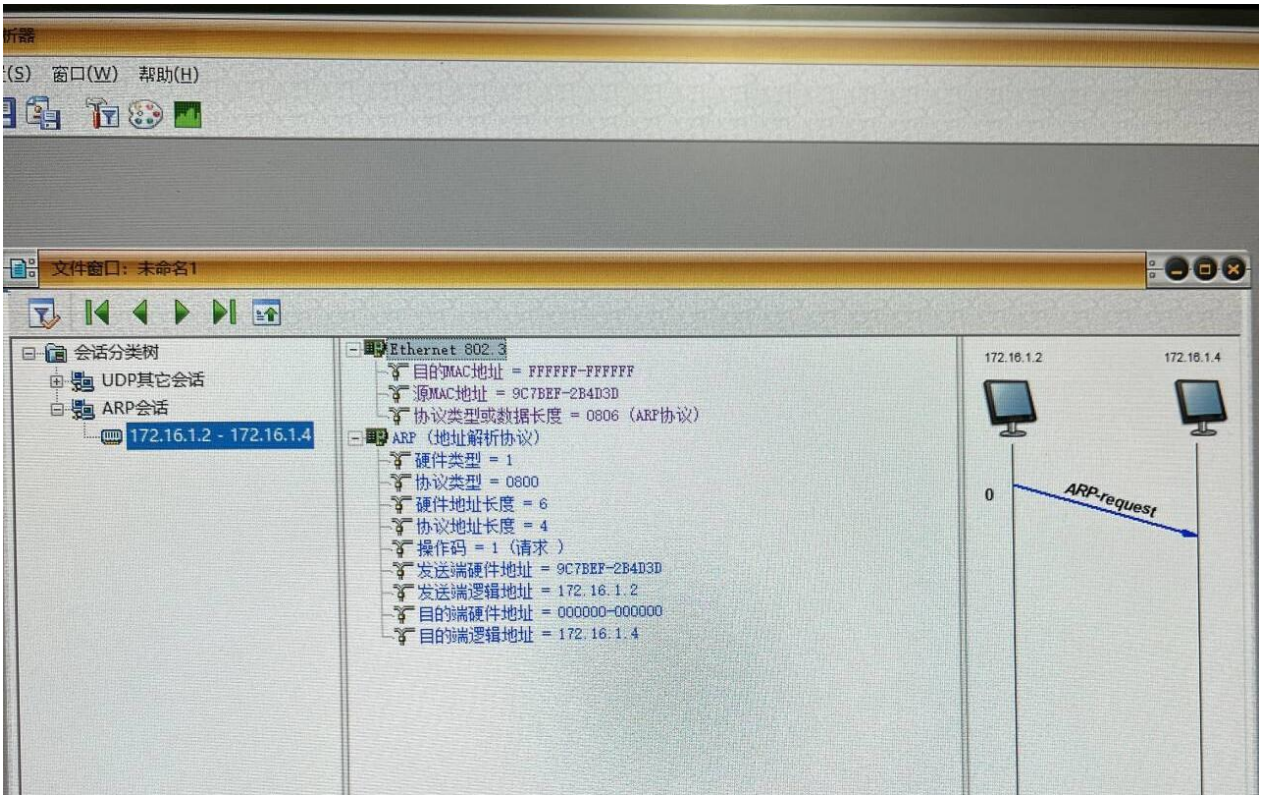
主机 F 收到的结果如下：


协议分析器 [文件窗口: 未命名4]
文件(F) 设置(S) 窗口(W) 帮助(H)
会话分类树
UDP其它会话
169.254.72.157 - 239.25
58003 - 1900
FF02::1:2 - FE80::DD44:9
ARP会话
172.16.0.1 - 172.16.0.2
172.16.0.1 - 172.16.0.3
172.16.0.2 - 172.16.0.3
Ethernet 802.3
目的MAC地址 = FFFFFF-FFFFFF
源MAC地址 = 9C7BEF-2B4D3C
协议类型或数据长度 = 0806 (ARP协议)
ARP (地址解析协议)
硬件类型 = 1
协议类型 = 0800
硬件地址长度 = 6
协议地址长度 = 4
操作码 = 1 (请求)
发送端硬件地址 = 9C7BEF-2B4D3C
发送端逻辑地址 = 172.16.0.3
目的端硬件地址 = 000000-000000
目的端逻辑地址 = 172.16.0.1
172.16.0.1
172.16.0.3
ARP-request
6
7
9
11
12
13
18
19
20
会话分析
协议解析


练习1
练习2
练习3
练习4
练习5
协议分析器 [文件窗口: 未命名4]
文件(F) 设置(S) 窗口(W) 帮助(H)
会话分类树
UDP其它会话
169.254.72.157 - 239.25
58003 - 1900
FF02::1:2 - FE80::DD44:9
ARP会话
172.16.0.1 - 172.16.0.2
172.16.0.1 - 172.16.0.3
172.16.0.2 - 172.16.0.3
Ethernet 802.3
目的MAC地址 = FFFFFF-FFFFFF
源MAC地址 = 9C7BEF-2ABA42
协议类型或数据长度 = 0806 (ARP协议)
ARP (地址解析协议)
硬件类型 = 1
协议类型 = 0800
硬件地址长度 = 6
协议地址长度 = 4
操作码 = 1 (请求)
发送端硬件地址 = 9C7BEF-2ABA42
发送端逻辑地址 = 172.16.0.2
目的端硬件地址 = 000000-000000
目的端逻辑地址 = 172.16.0.3
172.16.0.2
172.16.0.3
21
ARP-request
ARP-response
22
会话分析
协议解析

教务处制

主机 B 的结果如下：

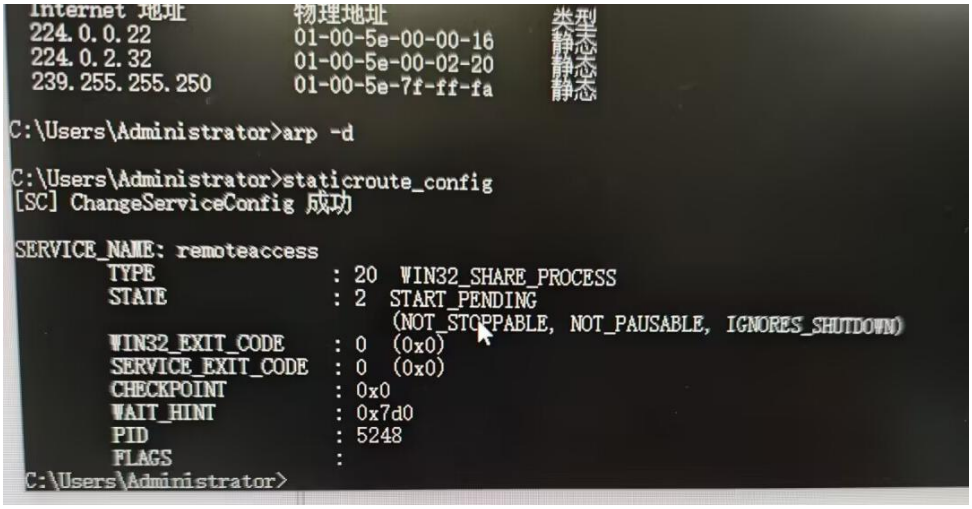


练习 3：跨路由地址解析（不同子网）

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1. 主机 B 在命令行方式下输入 staticroute_config 命令，开启静态路由服务。

主机 B 开启静态路由服务：



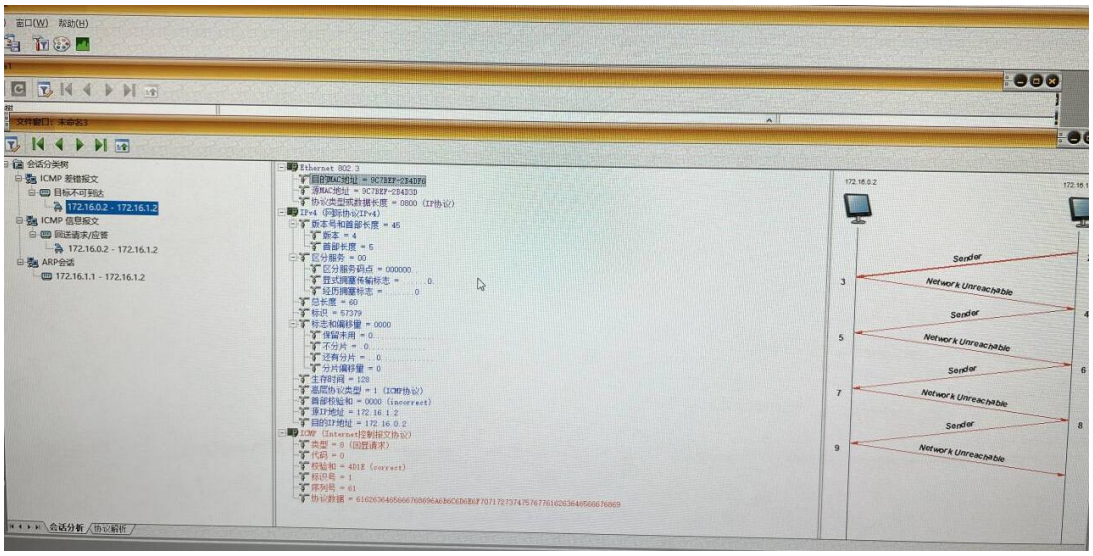
2. 主机 A、B、C、D、E、F 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。

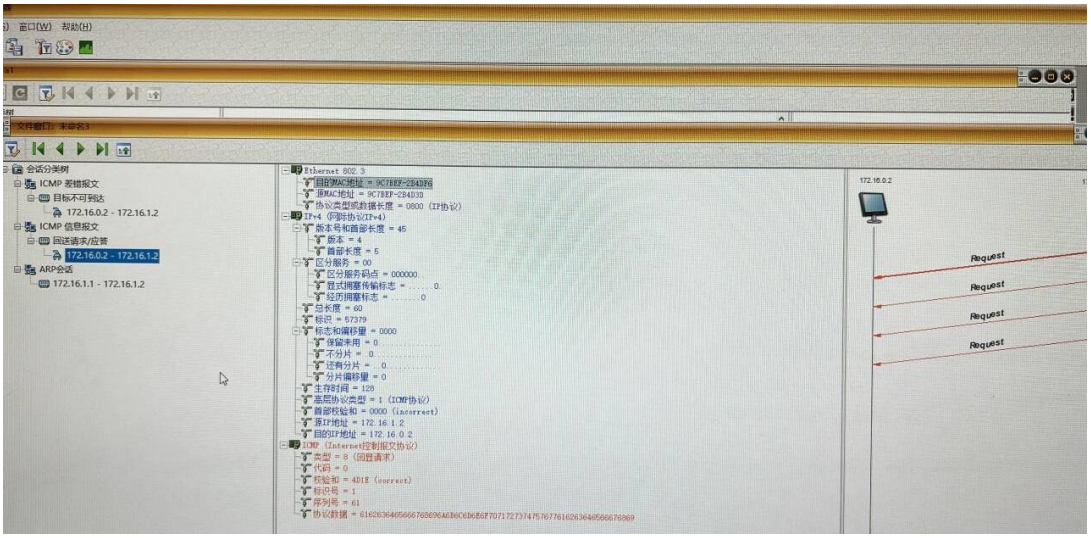
3. 主机 A、B、C、D、E、F 重新启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP、ICMP）。

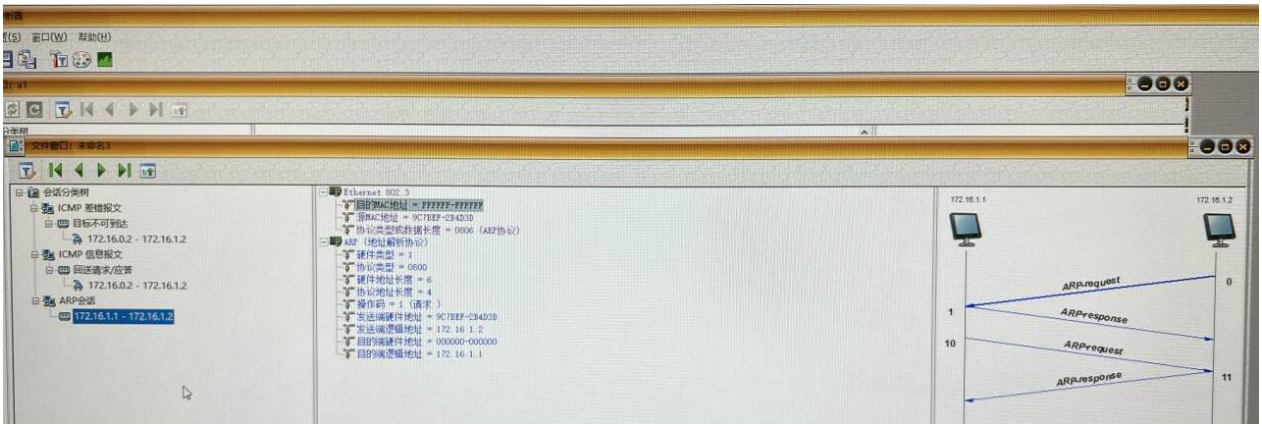
4. 主机 A ping 主机 E（172.16.0.2）。

5. 主机 A、B、C、D、E、F 停止数据捕获，查看协议分析器中采集到的 ARP 报文，并回答以下问题：

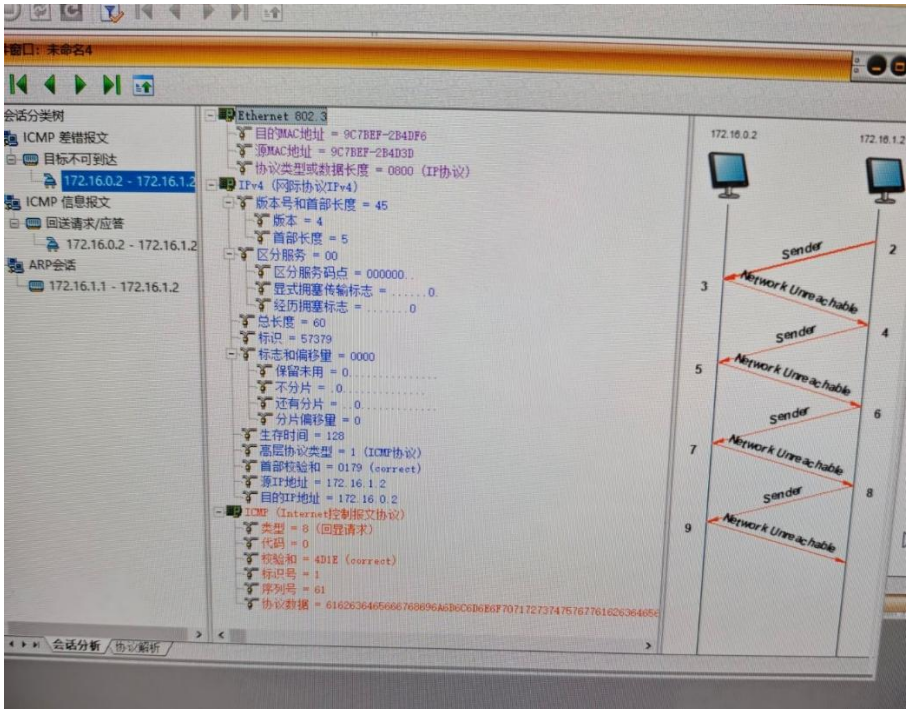
主机 A 协议分析器采集结果：

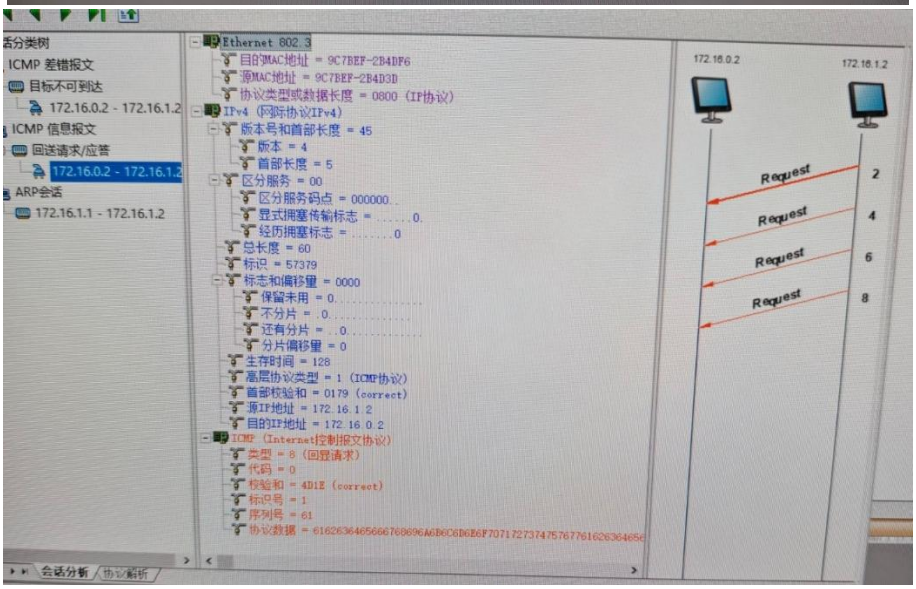




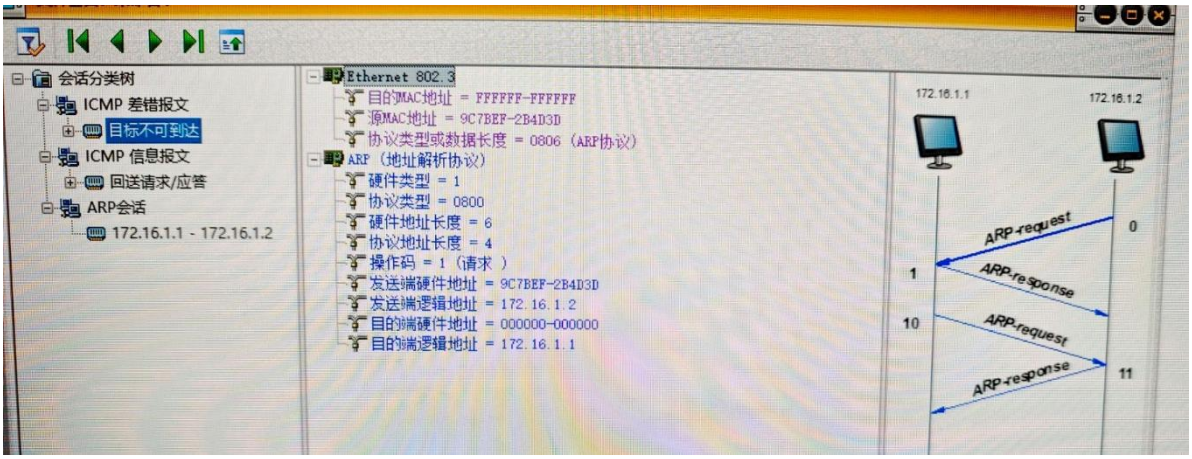


主机 B 协议采集器的结果如下:

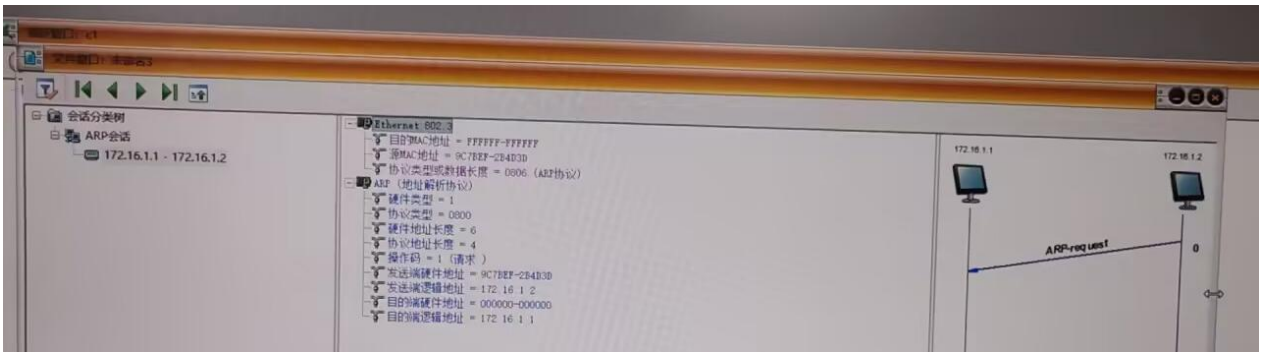




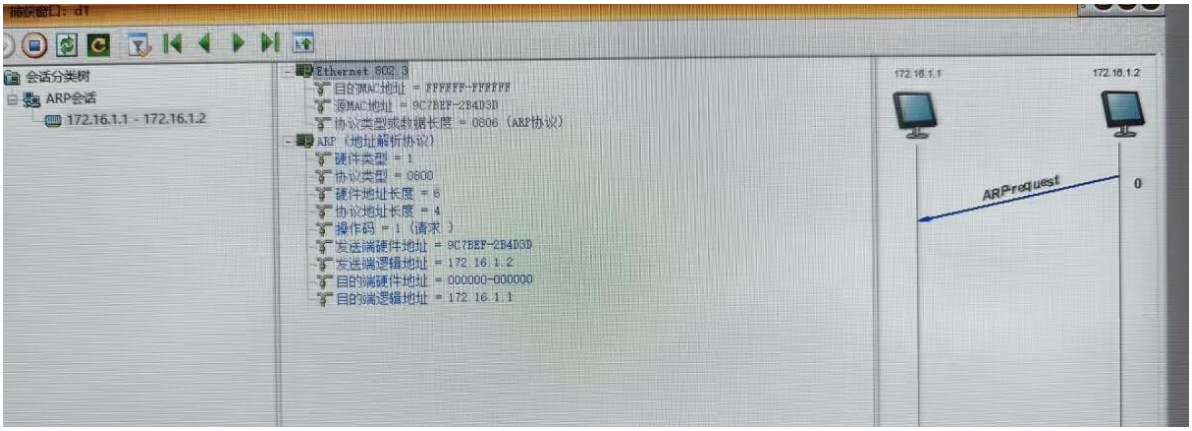
教务处制



主机 C 的协议采集器结果如下:

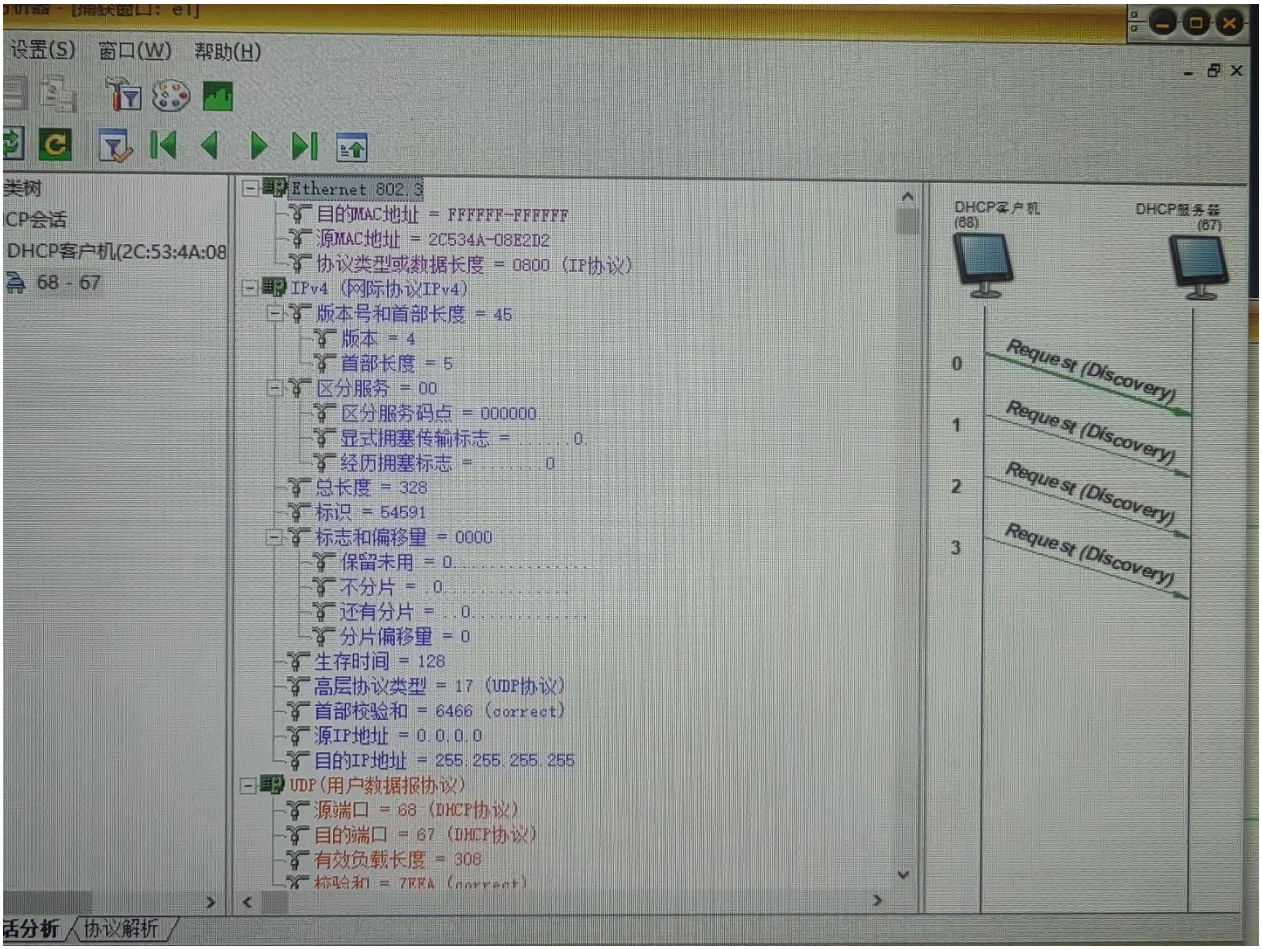


主机 D 的协议采集器结果如下:

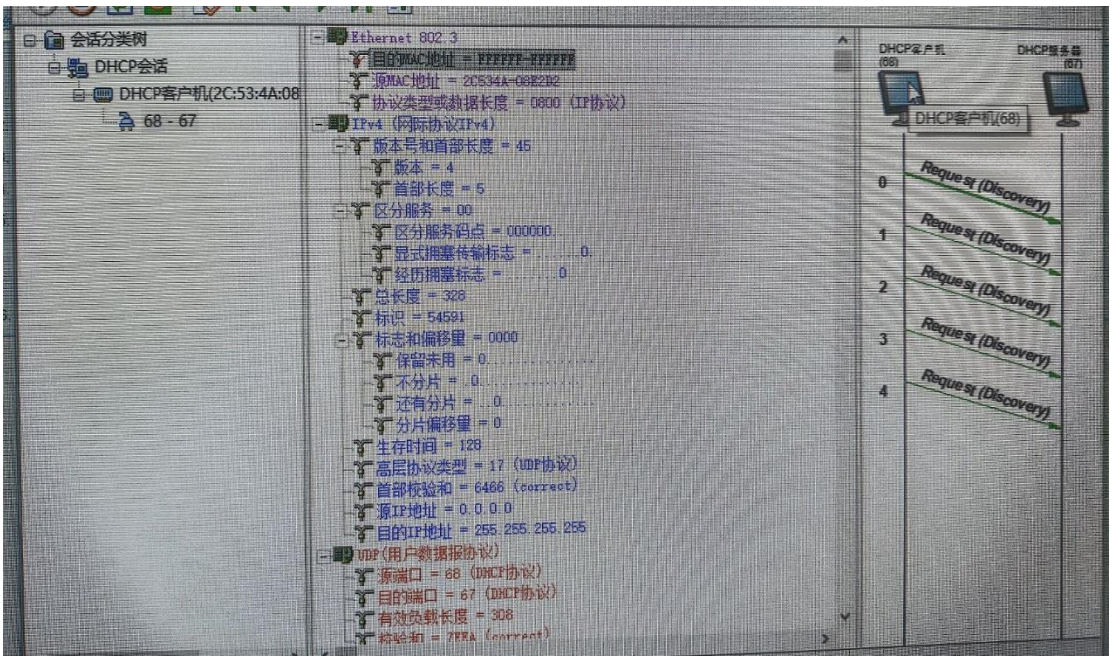


教务处制

主机 E 的协议解析器结果如下：



主机 F 的协议解析结果如下：



教务处制

● 单一 ARP 请求报文是否能够跨越子网进行地址解析？为什么？

答：不能。ARP（地址解析协议）是一个工作在数据链路层（第二层）的协议，它通过发送广播包（ARP 请求）来查找**同一本地子网**内的 IP 地址对应的 MAC 地址。路由器是连接不同子网的设备，它工作在网络层（第三层），并且**不会转发**第二层的广播包（如 ARP 请求）到其他子网，这是为了隔离广播域。因此，ARP 请求的范围被严格限制在它所发起的那个子网内部，它无法跨越路由器到达另一个子网。

三、 实验总结与收获

本次实验通过三个递进的练习，帮助我深入掌握了地址解析协议（ARP）的工作原理 、报文格式 以及 ARP 高速缓存的作用与维护过程 。在练习 1 和练习 2 中，通过在同一子网内执行 ping 命令 和手动构造并发送 ARP 请求报文 ，我观察了完整的 ARP 交互流程：当主机需要通信但缺少目标 MAC 地址时，它会先查询本地 ARP 缓存 ；若无记录，则在本地子网内广播一个 ARP 请求 ；目标主机收到请求后，会单播一个 ARP 应答 ；请求方收到应答后，将 IP 与 MAC 的映射关系写入本地缓存表 ，然后才能正常封装数据帧并发送。

实验的重点在练习 3，即跨子网的地址解析 。当主机 A（172.16.1.2）尝试 ping 不同子网的主机 E（172.16.0.2）时 ，协议分析器显示主机 A 并没有广播针对主机 E 的 ARP 请求 。相反，主机 A 判断出目标 IP 不在同一网段后，转而发送 ARP 请求以获取其默认网关（路由器 B，IP 为 172.16.1.1）的 MAC 地址 。同时，位于目标子网的主机 E 和 F 均未捕获到来自主机 A 的 ARP 请求 。这清晰地验证了 ARP 请求报文不能跨越子网的结论，因为 ARP 是数据链路层协议，其广播会被工作在网络层的路由器所隔离，路由器不会转发二层广播包 。